

TREND MICRO™

PC-cillin™ 2003

Complete Personal Virus Protection and Internet Security



Quick Start Guide

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes and the latest version of the Quick Start Guide, which are available from the Trend Micro Web site at:

www.trendmicro.com/download/documentation/

NOTE: A license to Trend Micro antivirus software includes the right to receive pattern file updates and technical support from Trend Micro or an authorized reseller, for one (1) year. Thereafter, you must renew Maintenance on an annual basis at Trend Micro's then-current Maintenance fees to have the right to continue receiving these services.

To order renewal Maintenance, you may download and complete the Trend Micro Maintenance Agreement at the following site:

www.trendmicro.com/license

Trend Micro, PC-cillin, PC-cillin for Wireless, MacroTrap, ScriptTrap and the Trend Micro t-ball logo are trademarks of Trend Micro Incorporated and are registered in certain jurisdictions.

All other brand and product names are trademarks or registered trademarks of their respective companies or organizations.

Copyright© 1995 - 2002 Trend Micro Incorporated. All rights reserved. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted without the express prior written consent of Trend Micro Incorporated.

Document Part No. PCEM01266/21014

Release Date: October 2002

Protected by U.S. Patent No. 5,951,698

The Quick Start Guide for Trend Micro™ PC-cillin 2003™ is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

Detailed information about how to use specific features within the software are available in the online help file and online Knowledge Base on the Trend Micro Web site.

At Trend Micro, we are always seeking to improve our documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com. Your feedback is always welcome. Please evaluate this document on the following site: www.trendmicro.com/download/documentation/rating.asp.

Contents

Chapter 1: Welcome to Trend Micro PC-cillin

What's New in PC-cillin 2003	1-2
Minimum System Requirements	1-4
Essential Getting Started Tasks	1-5
Installing PC-cillin	1-6
Registering Your Software	1-7
Updating PC-cillin	1-8
Hit the Ground Running... ..	1-10
What PC-cillin does "right out of the box":	1-10
What you can do with the click of a button:	1-11

Chapter 2: Getting to Know PC-cillin 2003

How PC-cillin Protects Your PC	2-2
Viewing the PC-cillin Main Window	2-3
Using the Standard mode	2-4
Using the Advanced mode	2-5
Viewing the Settings Window	2-7
Using the Real-time Agent	2-7
Starting the Real-time agent	2-8
Identifying Real-time agent icons	2-9
Viewing Logs	2-9
Introducing Outbreak Alerts	2-11
Accessing PC-cillin Online Help	2-11

Chapter 3: Protecting Your Files and Data

Best Practices for Safer Computing	3-2
Confirming Real-time Scan is Enabled	3-2
Confirming Email Scan is Enabled	3-3
Scanning Your Entire Computer	3-4
Scanning a Folder	3-4
Scanning a Single File	3-5
Running Scan Tasks	3-5
Searching for and Cleaning Trojans	3-6
Detecting Unknown Viruses	3-6

About ScriptTrap	3-7
About MacroTrap	3-7
Protecting Files on Your PDA	3-7
Starting Wireless Protection	3-8
Scanning for PDA Viruses	3-9

Chapter 4: Dealing with Viruses

What to do When a Virus is Detected	4-1
Actions on Uncleanable Files	4-2
Compressed files	4-3
Insufficient space or write-protected disks	4-3
Password-protected files	4-4
PE-type viruses	4-4
Creating Rescue Disks	4-4
Cleaning Boot Viruses	4-6
Understanding Viruses	4-7
Understanding Trojans	4-8

Chapter 5: Guarding Against Internet Attacks

Introducing the Personal Firewall	5-1
Installing and Enabling the Personal Firewall	5-2
Protecting Wi-Fi Connections	5-3
Halting Internet Traffic	5-4
Blocking Malicious Web Programs	5-5
WebTrap and the Personal Firewall	5-5
Filtering Unwanted Web Content	5-6

Chapter 6: Getting Support

Before Contacting Technical Support	6-1
Visiting the Trend Micro User's page	6-2
Visiting the Technical Support Web site	6-2
Contacting Technical Support	6-2
TrendLabs	6-3

Appendix

Upgrading Your Trial Version Software	A-1
Installing PC-cillin for Wireless	A-2
For Palm OS	A-2

For EPOC	A-3
For Pocket PC	A-3
Enabling and Configuring Proxy Settings	A-4
Removing PC-cillin	A-5
Removing PC-cillin for Wireless	A-5
For Palm OS	A-5
For Pocket PC	A-5
For EPOC	A-6



Welcome to Trend Micro™ PC-cillin™

Trend Micro PC-cillin 2003 provides complete virus protection and Internet security accessed through a simple interface. Responding to information from users, we have re-designed the interface to make it easier to accomplish any task. In this version we also introduce a unique Outbreak Alert service. This proactive service informs you in advance when a serious virus outbreak is occurring and prompts you to update PC-cillin to protect your computer from infection.

Wireless Ethernet (Wi-Fi) is becoming increasingly popular, so we have included a unique Wi-Fi Protection feature that is designed to help secure your wireless access points when connecting to a wireless network.

Re-built from the ground up, the Personal Firewall now tracks each connection and monitors the state of Internet connections. With the Personal Firewall, you can also control the security level, create exception rules, and view a list of Trojan ports. The result: a stronger, more flexible enhanced Personal Firewall.

WebTrap still offers solid protection from malicious scripts (Java or ActiveX programs), without causing a significant decrease in Web viewing time.

The Email Scan function has been expanded to include Webmail accounts. Now when you are accessing your Hotmail, AOL Mail, or Yahoo! Mail account with a browser, any attachment you try to download will be checked by PC-cillin.

We have also increased the ability to detect unknown viruses using advanced heuristic technology. Heuristic technology examines the "behavior" of files. While PC-cillin has been using heuristic technology for years, it now uses advanced heuristic technology which, unlike other antivirus software that only offer general heuristics, provides a customized heuristic scan to target specific virus file types. This makes detection more precise and powerful. Best of all, this technology is integrated with our scan engine and works automatically every time a scan is performed.

This chapter contains the following sections:

- What's New in PC-cillin 2003 on page 1-2
- Minimum System Requirements on page 1-4
- Essential Getting Started Tasks on page 1-5
- Installing PC-cillin on page 1-6
- Registering Your Software on page 1-7
- Updating PC-cillin on page 1-8
- Hit the Ground Running... on page 1-10

What's New in PC-cillin 2003

As viruses and other malicious programs become stronger and more clever, PC-cillin also continues to become more powerful to provide complete personal virus protection and Internet security.

This section describes the latest features added to Trend Micro PC-cillin:

Feature	Description
Outbreak Alert	PC-cillin offers a unique early warning service. This proactive service informs you in advance when a serious virus outbreak is occurring and prompts you to update PC-cillin to protect your computer from infection.
Email Scan	PC-cillin can scan messages and attachments retrieved from POP3 mail servers and attachments from Webmail servers (email that is stored on a server and accessed by a Web browser).
Wi-Fi Protection	With PC-cillin you can secure your wireless Ethernet access points with a click. This protects your computer when you are roaming in an untrusted area.
Enhanced Personal Firewall	Built from the ground up, the PC-cillin enhanced Personal Firewall provides solid protection to help prevent intrusion attempts from unauthorized users while you are connected to the Internet. The PC-cillin Personal Firewall is a stateful packet inspection firewall. Unlike packet filter firewalls, stateful packet inspection firewalls not only examine the headers of a packet, but also the contents.
Improved WebTrap	WebTrap has been enhanced to provide solid protection from malicious scripts (Java or ActiveX programs) without causing a significant decrease in Web viewing time.
Advanced Heuristic Technology	Unlike other antivirus software that only offers general heuristics, we provide a customized heuristic scan to target specific virus file types. Although PC-cillin has used heuristic technology for years, this advanced heuristic scan makes detection more precise and powerful.

Minimum System Requirements

You need the following minimum software and hardware to run PC-cillin.

Operating System:

- Microsoft™ Windows™ 98, 98SE, Me, NT Workstation 4.0 with Service Pack 6a, 2000 Professional with Service Pack 2, XP Home or Professional

CPU:

- Intel™ Pentium™ 166MHz or equivalent processor (or faster) for Windows 98, 98SE, Me, NT 4.0
- Intel Pentium 300MHz or equivalent processor (or faster) for Windows 2000, XP

Memory:

- 32MB of RAM (64MB or more recommended) for Windows 98, 98SE, Me, NT 4.0
- 64MB of RAM (128MB or more recommended) for Windows 2000
- 128MB of RAM for Windows XP

For all installations:

- Internet Explorer 4.01 or above
- 25MB of available hard disk space for installation
- WebTrap and Site filter supported browsers: Internet Explorer, Netscape Communicator 4.5 or later, Netscape 6 and 7, AOL browser
- Email Scan supported clients (for self configuration): Microsoft Outlook Express 4.0, Microsoft Outlook 98, Netscape Messenger 4.5, Eudora Pro 4.1

Note: Hardware requirement depends on your software environment. Internet connection is required to perform online registration, update, and other online services.

Essential Getting Started Tasks

This section provides a list of the most important tasks you have to complete to get up and running with PC-cillin. To effectively use PC-cillin and start protecting your PC, we strongly recommend you perform all of these tasks.

Task	Topic
Install the software	Installing PC-cillin on page 1-6 , (if you have a PDA, refer to <i>Installing PC-cillin for Wireless</i> on page A-2 of the Appendix)
Register PC-cillin	Registering Your Software on page 1-7 , if you don't register you are unable to update; PC-cillin needs to update to stop the latest viruses (if you need to upgrade from the 30-day trial version, refer to <i>Upgrading Your Trial Version Software</i> on page A-1 of the Appendix)
Perform a Manual Update	Updating PC-cillin on page 1-8 , since new viruses are constantly being discovered, we strongly recommend you regularly update PC-cillin (to automatically let PC-cillin search for and download updates, enable Intelligent Update)
Manually Scan all files	Scanning Your Entire Computer on page 3-4 , perform a complete scan of your computer to ensure there are no viruses or other malicious programs hiding on your PC

Installing PC-cillin

Installing PC-cillin is simple and only takes a few minutes. During the installation process you are given the choice to install the Personal Firewall. If you do not install the Personal Firewall, other features will also not be installed including Wi-Fi Protection, Internet traffic status, and the ability to instantly halt Internet traffic.

Important: Before installation, you must remove any existing antivirus software including previous versions of PC-cillin or any other Trend Micro antivirus software.

To install PC-cillin:

1. Insert the PC-cillin program CD into your CD-ROM drive, and do the following:
 - If the menu automatically appears, click **Install PC-cillin**, and then click **Next**.
 - If the installation program doesn't automatically start, click **Start** > **Run**. In **Open**, type D:\Setup\setup.exe and click **OK** (where D:\ is the drive letter of your CD-ROM). Click **Next**.
2. Click **I accept the terms of the license agreement** to accept and continue installing PC-cillin. The installation procedure will quit if you do not accept the terms.
3. Click **Next**. PC-cillin scans your system memory, boot sector, and critical files before installing the program files. If PC-cillin finds an infected file or Trojan, it cleans or deletes it. The **Customer Information** screen appears. Do the following:
 - In **User Name**, type a user name. You must provide a user name to continue installation.
 - In **Organization**, type the name of your organization.
 - In **Serial Key**, type your serial key. If you do not have a serial key, you can continue installation and install a 30-day trial version. If you want to install the trial version, an additional screen appears when you click **Next** giving you the option to install it. Select the **I want to install the 30-day trial version** check box, and then click **Next**. With this

version you will not be able to register or update and after 30 days virus scanning will be disabled--you should either purchase the product or remove it.

4. Click **Next**. The **Destination Folder** screen appears. You can choose where PC-cillin will be installed or use the default location. To change the location click **Change**, and then browse to the desired location.
5. Click **Next**. The **Install the Personal Firewall** screen appears. To install the Personal Firewall, click **Next**. To continue installation without installing the Personal Firewall, clear the **Install the Personal Firewall** check box, and then click **Next**.
6. If you are ready to complete installation, click **Install**. If you want to make changes, click **Back** to navigate to the screen where you want to make your changes.
7. Click **Finish**.

Registering Your Software

Take a few minutes to register your software online and receive the benefits. A license to Trend Micro antivirus software includes the right to receive pattern file updates and technical support from Trend Micro or an authorized reseller, for one (1) year. Thereafter, you must renew Maintenance on an annual basis at Trend Micro's then-current Maintenance fees to have the right to continue receiving these services.

Important: You must register your software before you can perform updates. You need to perform updates to keep your computer protected.

To register your software:

1. Make sure you are connected to the Internet.
2. On the PC-cillin Main window, click **Register**. The **Register Now** screen appears.
3. Confirm that your full version serial number already exists and click **Register Now**. The Register Web page loads in your browser.

4. On the Register Web page, type your name, email address, and other required information in the appropriate fields.
5. Click **Preview**. Confirm the information you entered is correct.
6. Click **Submit**. A Confirmation Web page loads with the License Key. The License Key is sent to the email address you just typed and appears under **Step 3** on the PC-cillin Main window **Register Now** screen. If the License Key doesn't appear on the **Register Now** screen, copy it from the Web page or email and paste it under **Step 3**.
7. Click **Finish**.

Congratulations! You have registered your software. You can now use the full functionality of PC-cillin 2003 and receive the benefits.

Note: If you have trouble connecting to the Internet you may need to configure your proxy settings. Refer to [Enabling and Configuring Proxy Settings](#) on page A-4 in the Appendix for instructions.

Updating PC-cillin

To protect your computer against the latest threats, you need to regularly update your program files, scan engine, and virus pattern files. Although all components can be updated, pattern files are updated on at least a weekly basis. Updating your pattern file provides you with the most up-to-date protection and lets PC-cillin scan for the latest viruses or other malicious programs.

Important: Since hundreds of new viruses are discovered every month, we strongly recommend you regularly update PC-cillin.

In addition, as new viruses appear, and existing ones evolve, it becomes necessary to update certain program files and add new functionality to the scan engine. Updating your scan engine ensures PC-cillin can act on the new instructions in the virus pattern to detect and remove viruses.

Note: Before you can update PC-cillin you must register your software.

To perform a manual update:

1. On the PC-cillin Main window, under the **Standard** or **Advanced** tab click **Update Now**. The **Update Now** screen appears. If the Update process doesn't begin click **Update**. The meter displays the update progress.
2. If you need to halt the update, click **Stop**. To continue updating, click **Update**.

To automatically search for and download the latest pattern, and program files from the Trend Micro ActiveUpdate server, we recommend you schedule the Intelligent Update function. This powerful function keeps PC-cillin and all its components updated to offer you maximum protection with minimum user intervention.

To perform a scheduled update:

1. On the Settings window, click **Program Update**.
2. Make sure the **Enable Intelligent Update...** check box is selected.
3. Select how often you want PC-cillin to check for updates.
4. Click **Apply**.

Note: To allow PC-cillin to automatically perform updates without asking permission, under **Update Alert**, select the **Automatically update without alerts** check box.

Hit the Ground Running...

Even before you completely install PC-cillin, it checks your main system files for viruses and Trojan horse programs. Then after it's installed, PC-cillin helps keep your computer free from infection with a series of pre-defined automated tasks.

What PC-cillin does "right out of the box":

Without having to configure anything, PC-cillin will perform the following:

- Check for viruses every time you open, copy, move, or save a file
- Protect against downloading infected files
- Detect and cleans Trojans
- Scan your email message and attachments as they are being downloaded from the POP3 email server (if you use the email clients: Microsoft™ Outlook™ 98 or above, Outlook Express 4.0 or above or Eudora™ Pro 4.0 or above). Also scan Webmail attachments and they are being downloaded from a Webmail server (a Webmail server is accessed by a Web browser for example, Microsoft Hotmail™, Yahoo!™ Mail, and AOL™ Mail)
- Protect your computer against attacks from the Internet (only if the Personal Firewall has been installed)
- Monitor your Microsoft Word™ and Excel™ sessions for macro viruses, using MacroTrap™, a system that detects macro viruses through heuristics, rule-based methods, rather than pattern matching
- Check for unknown viruses based on their “behavior”, using advanced heuristic technology
- Scan all files on your hard drive according to a default scheduled scan task
- Scan all program files for viruses according to a default scheduled scan task

What you can do with the click of a button:

- Scan every file on your system
- Scan any file from Windows Explorer or My Computer by right-clicking the file icon
- Scan floppy disks
- Check all Word or Excel documents for macro viruses



Getting to Know PC-cillin 2003

This chapter contains sections that help you become familiar with Trend Micro PC-cillin 2003. In addition, it introduces Outbreak Alerts and describes how to access the PC-cillin online help.

Included in this chapter are the following sections:

- How PC-cillin Protects Your PC on page 2-2
- Viewing the PC-cillin Main Window on page 2-3
- Viewing the Settings Window on page 2-7
- Using the Real-time Agent on page 2-7
- Viewing Logs on page 2-9
- Introducing Outbreak Alerts on page 2-11
- Accessing PC-cillin Online Help on page 2-11

How PC-cillin Protects Your PC

PC-cillin is designed to protect your computer from both external and internal threats.

Threat	PC-cillin Protection
External: viruses and other malicious programs (for example, Trojans, worms), infected email	<p>Real-time Scan detects and scans any file downloaded, copied or moved to your computer.</p> <p>Email Scan provides protection from infected POP3 email messages and attachments and infected Webmail (Hotmail, AOL Mail, Yahoo! Mail) attachments.</p>
Internal (local machine): viruses and other malicious programs (for example, Trojans, worms)	<p>Manual Scan and scheduled scan tasks check your local machine.</p> <p>Trojan Ports block a list of ports used by known Trojan attacks. Many backdoor Trojan attacks can be avoided by preventing access to these ports.</p> <p>PC-cillin detects the activity of Trojan horse programs, recovers system files that are modified by Trojans, stops their processes, and deletes files left behind by Trojans.</p>
Virus Outbreaks	<p>Outbreak Alert proactively warns you of an outbreak or other high-risk situation and advises you to update PC-cillin.</p> <p>Instantly halt all Internet traffic if you suspect an outbreak or other suspicious activity.</p>
Malicious Hackers	<p>A stateful inspection firewall built from the ground up provides solid protection from outside intruders and exception rules for flexibility.</p>
Wireless LAN Intrusion	<p>Wi-Fi Protection helps secure your computer when accessing an untrusted wireless LAN environment.</p>

Malicious Web programs	WebTrap blocks malicious script attacks designed to run on Web sites and cause harm to visitors.
Inappropriate Web sites	Site Filter lets you block inappropriate Web sites from loading.
PDA viruses	PC-cillin for Wireless.

Viewing the PC-cillin Main Window


Designed for the home or small office user, the program's friendly interface quickly gives you access to and familiarizes you with the powerful features of PC-cillin 2003. The tab interface includes a Standard and Advanced mode that lets you easily switch between the two modes.

The Standard mode is ideal for users who are just getting started with antivirus and Internet security. When you want more control and access to advanced functions, just switch to the Advanced mode.

The PC-cillin Main window provides the interface to rapidly execute your actions. On the PC-cillin Main window, you can view both Standard and Advanced modes and the menu bar.

To view the PC-cillin Main window:

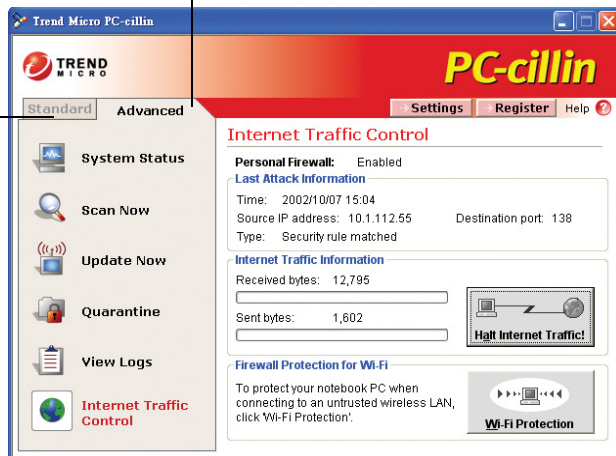
- Click **Start > Programs > Trend Micro PC-cillin 2003 > PC-cillin 2003**.

Tip: In the system tray, right-click the Real-time agent  and click **Open Main**.

The PC-cillin Main window appears:

Advanced tab- Click to view the Advanced mode and perform advanced PC-cillin functions

Standard tab- Click to view the Standard mode and quickly perform common PC-cillin tasks






Using the Standard mode

Ideal for users new to antivirus and security, the Standard mode lets you access the following commonly used functions: viewing the system status, scanning all drives, and updating your software.

To view the Standard mode:

On the PC-cillin Main window, click the **Standard** tab. The Standard mode menu appears.








To perform the following action:	Click:
View the system status.	
Scan all drives for infected files that are connected to your computer.	
Check the Trend Micro ActiveUpdate server for the latest components.	

Using the Advanced mode

The Advanced mode menu lets you perform advanced PC-cillin functions including viewing your system status, selectively scanning drives or folders, managing quarantined files, and viewing logs. In the Advanced mode, as in the Standard mode, you can also update your software. In addition, if you have installed the Personal Firewall, you can also view Internet traffic information, halt all Internet traffic, and enable Wi-Fi Protection.

To view the Advanced mode:

- On the PC-cillin Main window, click the **Advanced** tab. The Advanced mode menu appears.

To perform the following action:	Click:
View the system status.	
Select the drives or folders you want to scan.	
Check the Trend Micro ActiveUpdate server for the latest components.	
View and manage quarantined files or access the Quarantine Guide.	
View logs for all update, virus, Site filter, and Personal Firewall activity.	
 View and control Internet traffic or enable Wi-Fi Protection.	



Personal Firewall must be installed to perform this action.

Viewing the Settings Window

The Settings window provides a friendly interface to configure PC-cillin functions.

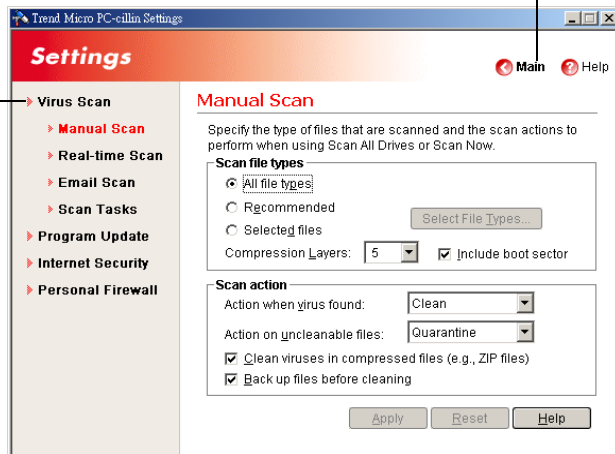
To view the Settings window:

- Click **Start > Programs > Trend Micro PC-cillin 2003 > PC-cillin 2003 Settings**. The Settings window appears.

Tip: In the system tray, right-click the Real-time agent  and click **Settings**.

Click the links to display the screens you want to configure. For most links the menu expands to display submenu items

Click to display the Main window



Using the Real-time Agent

The Real-time agent is the quickest way to access certain functions, for example to display the Main or Settings window.



Starting the Real-time agent

When the PC-cillin program loads, the Real-time agent should automatically launch and appear in your system tray. However, if you do not see the Real-time agent in your system tray, we recommend you launch it.

To start the Real-time agent:

- Click **Start > Programs > Trend Micro PC-cillin 2003 > Real-time Agent**.

With the Real-time agent, you know at a glance if Real-time Scan is enabled or disabled.





To:	Do the following:
Open the Main window	Double-click the Real-time agent.
Open the Settings window	Right-click the Real-time agent and click Settings .
Turn off the Real-time agent	Right-click the Real-time agent and click Exit . Important: If you turn off the Real-time agent, Real-time Scan will also be disabled.
 Halt all Internet Traffic	Right-click the Real-time agent and click Halt all Internet Traffic! .
 Enable Wi-Fi Protection	Right-click the Real-time agent and click Wi-Fi Protection .



Personal Firewall must be installed to perform these actions.

Identifying Real-time agent icons

Use the table below to learn the meanings of Real-time agent icons.

Icon	Description
	All incoming and outgoing Internet traffic has been stopped (to allow Internet traffic, refer to <i>Halting Internet Traffic</i> on page 5-4)
	Connecting to the Trend Micro server to download the latest updates
	Real-time Scan is enabled
	Real-time Scan is disabled (to enable Real-time Scan, refer to <i>Confirming Real-time Scan is Enabled</i> on page 3-2)

Viewing Logs

PC-cillin keeps logs for all update, virus, Site filter, and Personal Firewall events. These logs can be viewed from the View Logs screen and provide a valuable source of information. For example, you can view Virus logs to find out if a detected virus is a Trojan or worm and should be deleted rather than quarantined.

In addition to displaying the date and the time of each recorded log, the various log types provide log-specific information.

Log	Entries are created when:
Update	You try to download the latest components. Update log entries also contain what file(s) were downloaded and installed from Trend Micro and the status—Successful or Unsuccessful—of the download.
Virus	A virus or other malicious program is detected. Virus log entries also contain the time the virus was detected; the type of scan—Real-time or Manual—that detected the virus, the source type of the virus, the name of the virus, the name of the file that contains the virus, the status of the first action, and if applicable the status of the second action.
Site Filter	A Web site is blocked or harmful Web content is encountered. Site filter log entries also contain the time access to a restricted site was attempted, the URL, or Web address that was blocked, and the action Site filter performed.
Personal Firewall	Your computer experiences an attack from the Internet. Personal Firewall log entries also contain the type of firewall defense, time of the attack, direction of network traffic, type of protocol used, source IP address, source port number, destination IP address, destination port number, and the reason traffic was blocked.

To view a log:

1. On the PC-cillin Main window under the **Advanced** tab, click **View Logs**.
2. Under **Log Type**, click the type of log you want to view.
3. Click **View Logs**.
4. Select the date of the log you want to view.



5. To sort the logs (ascending or descending) by column header (for example: Time), click the column title for the desired display.

Introducing Outbreak Alerts

PC-cillin includes an innovative, proactive service to protect you in advance against the latest virus outbreaks or other malicious threats. Leveraging the research and knowledge of Trend Micro TrendLabs, PC-cillin can proactively warn you in advance of threats so you have time to update your software to prevent infection.

Outbreak Alerts are classified as Red and Yellow Alerts. Red Alerts correspond to the TrendLabs High-Risk ranking and Yellow Alerts to the Medium-Risk ranking.

Important: If you receive an Outbreak Alert, we strongly recommend you immediately update PC-cillin.

 High-Risk Criteria (Red Alert)	 Medium-Risk Criteria (Yellow Alert)
<p>Several infection reports reporting rapidly spreading malware.</p> <p>The industry's first 45-minute Red Alert solution process is started: An official pattern release (OPR) is deployed with notification of its availability, any other relevant notifications are sent out</p>	<p>Infection reports are received from several business units (BUs) as well as support calls confirming scattered instances, and an OPR is made available for download.</p>

Accessing PC-cillin Online Help

The PC-cillin online help provides comprehensive coverage of all the functions and features of PC-cillin 2003. Use the PC-cillin online help to find the answers for your PC-cillin questions.

To access PC-cillin online help:

- On the PC-cillin Main or Settings window, click **Help > Trend Micro PC-cillin Help**. The online help appears.

In addition, when you are using the program you may also see Help buttons. Click these buttons to view context-sensitive help (relevant help information based on what you are currently viewing).



Protecting Your Files and Data

This chapter contains information about basic tasks you should perform to protect your computer. It includes the following sections:

- Best Practices for Safer Computing on page 3-2
- Confirming Real-time Scan is Enabled on page 3-2
- Confirming Email Scan is Enabled on page 3-3
- Scanning Your Entire Computer on page 3-4
- Scanning a Folder on page 3-4
- Scanning a Single File on page 3-5
- Running Scan Tasks on page 3-5
- Searching for and Cleaning Trojans on page 3-6
- Detecting Unknown Viruses on page 3-6
- Protecting Files on Your PDA on page 3-7

Best Practices for Safer Computing

Take the following proactive measures to prevent your computer from becoming infected.



Make sure Real-time Scan is enabled- Real-time Scan provides constant protection against viruses. With Real-time Scan enabled, you significantly reduce the chance of your computer becoming infected. Because it is so powerful (and because it operates imperceptibly in the background), we recommend that you always keep Real-time Scan enabled.



Update PC-cillin- Register your software and download the latest versions of the PC-cillin pattern files, scan engine, and program components to ensure PC-cillin uses the latest antivirus technology. You should also schedule PC-cillin to automatically perform updates using Intelligent Update.



Beware of suspicious email attachments- Email is the most common way viruses and malicious code spread. If you receive an email from someone you don't know, you shouldn't save or run any files attached to the email. However, regardless of who sent you the email, be suspicious of email attachments that contain executable files (.exe, .com).



Set scheduled scan tasks- Scan tasks are a quick and easy way to schedule a variety of Manual Scans. Using scan tasks lets you configure the type of files to search and how often to perform the scan. For example, you could set a scan task to scan all types of files on your computer, every Friday night at 10:00 PM.



Keep informed- Regularly visit the Trend Micro Web site (www.trendmicro.com) for the latest virus information and security alerts. In addition, you can learn more about viruses by accessing the online Trend Micro Virus Encyclopedia.



Update Microsoft Windows - Microsoft responds to security issues in their software by releasing patches and other updates on their Web site. Microsoft Windows operating systems provide a Windows update function that allows you to easily download and update these files.

Confirming Real-time Scan is Enabled

Real-time Scan provides constant protection against viruses by scanning files that are copied, downloaded, or moved to your computer. Real-time scanning

takes place in the background and requires no user intervention, so you don't really have to do anything to "use" Real-time Scan--just be sure it is enabled.

To quickly identify whether Real-time Scan is enabled (which it is by default), check the Real-time agent in the system tray.



Enabled (default)



Disabled

If Real-time Scan is disabled, we strongly recommend you enable it.

Important: If you turn off the Real-time agent, Real-time Scan will also be disabled.

To enable Real-time Scan:

- In the system tray, right-click the Real-time agent, and then click **Real-time Scan**.

Confirming Email Scan is Enabled

Email is the most common way for viruses and other malicious programs to spread and opening an infected email or attachments is the primary means of virus infection. Due to the popularity of email communication, virus writers create viruses that exploit the vulnerabilities of email client software.

Email Scan is designed to check mail messages and attachments downloaded from an Internet (POP3) mail server. Examples of supported email clients that use POP3 mail servers include Microsoft Outlook 98 and above, Outlook Express 4.0 and above, Eudora Pro 4.1 and above, and Netscape Messenger 4.5 and above.

Email Scan can also scan mail attachments downloaded from a Webmail account (email stored on a server and accessed by a Web browser) including Microsoft Hotmail, Yahoo! Mail, and AOL Mail.

The Email Scan feature must be enabled on the computer before accessing the email server.

To confirm Email Scan is enabled:

1. On the Settings window, click **Virus Scan**.
2. Click **Email Scan**.
3. Make sure both the **Enable incoming mail scanning (POP3 mail)** and **Enable Webmail scanning** check boxes are selected. If they are not, select them.
4. Click **Apply**.

Scanning Your Entire Computer

Scan all drives to check if your computer is infected. With one click, PC-cillin provides a fast and easy way to scan all drives connected to your computer for infected files.

To scan your entire computer:

- On the PC-cillin Main window under the **Standard** tab, click **Scan All Drives**. The Scan Files dialog box appears and PC-cillin begins scanning. To stop scanning, click **Stop**. A confirmation message box appears. Click **Yes** to stop.

Note: PC-cillin scans the file types and executes the necessary scan actions according to the Manual Scan settings. To change these settings, refer to the online help under the book "Changing PC-cillin Settings".

Scanning a Folder

With PC-cillin, you can scan the entire contents of a folder, including subfolders. PC-cillin scans the file types and executes the necessary virus actions according to the Manual Scan settings.

To scan a folder:

- Right-click the folder, and then click **PC-cillin**.

Tip: You can also "drag" the folder onto the PC-cillin Main window.

Scanning a Single File

PC-cillin can easily run a quick scan of any file. PC-cillin scans the file types and executes the necessary virus actions according to the Manual Scan settings.

To scan a single file:

- Right-click the file, and then click **PC-cillin**.

Tip: You can also right-click the file, and then click **Properties**. Click the **Virus Property** tab or you can "drag" the file onto the PC-cillin Main window.

Running Scan Tasks

Scan tasks let you schedule a variety of scans to automatically run at the specified time. For example, you could create a scan task that checked all file types on all your drives, every Friday at 10:00 PM. However, at any time you can manually execute previously defined scan tasks.

PC-cillin 2003 provides a number of pre-defined scan tasks. In addition to running these scan tasks, you can also view them to give you hints about how to create your own effective scan tasks.

To run a scan task:

1. On the PC-cillin Main window under the **Advanced** tab, click **Scan Now**.
2. Under **Scan tasks**, select the task you want to execute.

3. Click **Execute**. To stop scanning, click **Stop**. A confirmation dialog box appears. Click **Yes** to stop.

Note: To learn more about scan tasks, refer to the online help under the book "Managing Scan Tasks".

Searching for and Cleaning Trojans

Traditional antivirus products only scan "files"; they open files and check for virus code. But they don't check and clean system files and can't clean or delete Trojan horse programs (also known as Trojans) if they have already run in the system. PC-cillin detects Trojan activity, recovers Trojan modified system files, stops Trojan processes, and deletes files left behind by them.

PC-cillin automatically searches for Trojans during initial installation, and every time Real-time Scan starts. However, you can also manually search for Trojans.

To manually search for and delete Trojans:

1. Locate the folder where you installed PC-cillin 2003 (for example, the default location is C:\Program Files\Trend Micro\PC-cillin 2003).
2. Double-click the **Tsc.exe** file.

Detecting Unknown Viruses

In addition to searches based on pattern files, PC-cillin also uses advanced heuristic technology to help detect unknown viruses. Heuristic Technology examines the "behavior" of files. This core technology has already been integrated in PC-cillin for years. Unlike our competitors that only offer general heuristics, we provide a customized heuristic research to target specific virus file types. This makes detection more precise and powerful.

Best of all, because this technology is integrated with our scan engine and works automatically every time a scan is performed.

About ScriptTrap™

With the addition of ScriptTrap technology, PC-cillin not only guards against harmful known script-based viruses ("ILOVEYOU" and "Anna Kournikova"), but can also protect your PC from new, unknown script-based threats. Using the following processes, ScriptTrap automatically scans for scripting viruses based on "what they do" rather than how they are written:

- lexical analysis- divides the script's source code into components, called tokens, based on punctuation and other keys
- semantic parsing- attempts to determine the meaning of each component

About MacroTrap™

In 1996 Trend Micro developed MacroTrap—combined pattern and intelligent rules-based virus scanning technology—which searches for and removes both and unknown macro viruses.

The Trend Micro patented MacroTrap technology works through:

- Pattern-match scanning to detect known macro viruses combined with intelligent, rules-based heuristic scanning for detecting unknown macro viruses.
- Maximizing scanning efficiency by extracting only files' macro-carrying segments from the OLE2 data file structure, which minimizes scanning time and CPU processing overhead.

MacroTrap is platform-independent scanning technology that boosts the macro virus detection and removal rates in all Trend Micro antivirus software products well over that of traditional pattern-matching methods alone.

Protecting Files on Your PDA

PC-cillin for Wireless™ is very easy to use; the main screen features three buttons, Scan, Log, and Virus Info. These three features are standard features for all PC-cillin for Wireless versions and are discussed in greater detail in later sections.

The main screen also shows version information about the scan engine and the pattern file installed on your PDA. You will always know the condition of your virus protection, each and every time you start up.

Starting Wireless Protection

Depending on the type of PDA you have, refer to the appropriate instructions.

For Palm OS

1. Go to the Palm main screen and make sure it is set to show all applications.
2. To start the program, tap **PC-cillin**.

Enabling Real-time Scan (For Palm OS)

Real-time Scan prevents viruses that enter the device from every possible entry point - beaming, synching, email and Internet downloading. Real-time Scan activates whenever applications on the device are launched and prevents viruses from activating on the device.

Real-time Scan for Palm has a separate user interface and a separate icon.

To enable Real-time Scan:

1. Go to the Palm main screen and make sure it is set to show all applications.
2. Tap **RealTime**.
3. Select the **Enable Real-time Scan** check box.
4. Tap **Apply**.

For Pocket PC

1. Tap **Start** in the upper-right corner of the screen. The Start menu appears.
2. Tap **PC-cillin**.

For EPOC

1. Tap **Extras** to show the *Extras* Bar.

2. Tap **PC-cillin** to start the program.

Scanning for PDA Viruses

To scan for viruses, simply tap **Scan**. If viruses are detected on your PDA, the names are displayed after completion of the scan.

The number of files scanned and viruses found is also displayed.

Dealing with PDA Viruses

If a virus is detected on your PDA, you can perform the following actions:

- To delete all detected viruses, tap **Delete All**.
- To delete only selected viruses, choose the target virus on the list of detected viruses, and tap **Delete**.
- To take no action against the detected viruses, tap **Back** to return to the program's entry screen.

Important: If you tap **Back**, the virus remains on your PDA.

Getting PDA Virus Information

Virus information can be viewed either from the main screen, or on the scan results screen.

From the Main Screen:

1. Tap **Virus Info**. The virus encyclopedia appears.
2. Select the virus you want to know more information about.
3. Tap **Description** to view the virus description.

From the Scan Results Screen:

1. Select the virus you want to know more about from the list of detected viruses.
2. Tap **Description** to view the virus description.



Dealing with Viruses

With the amount of viruses already “in-the-wild” and the number of viruses created and released, it is very likely you will encounter a virus. The following sections are described in this chapter:

- What to do When a Virus is Detected on page 4-1
- Actions on Uncleanable Files on page 4-2
- Creating Rescue Disks on page 4-4
- Cleaning Boot Viruses on page 4-6
- Understanding Viruses on page 4-7
- Understanding Trojans on page 4-8

What to do When a Virus is Detected

When PC-cillin detects a virus either by Real-time, Manual, or Email Scan, PC-cillin notifies you of the virus and the scan action performed.

For Real-time and Email Scan a message box will appear describing the infected file and the scan action performed.

The scan actions for Real-time, Manual, or Email Scan depend on the settings you have configured for each scan. However, the default action for all scans is Clean.

This simply means if a file becomes infected, PC-cillin first attempts to clean the file. The default secondary action for Real-time and Manual Scan is Quarantine.

If PC-cillin detects an uncleanable file or a malicious program, which due to their nature can't be cleaned (Trojans, worms), the file or program is moved to the Quarantine folder where it can't cause any harm or further infection. For Email Scan the default secondary action is Delete.

Actions on Uncleanable Files

If you haven't changed any settings, you don't need to do anything. We strongly recommend you use the default values for uncleanable files. The default secondary scan action for Real-time and Manual Scan is Quarantine. This simply means that if PC-cillin detects an uncleanable file or a malicious program such as a Trojan or worm, the file or program is moved to the Quarantine folder.

Any infected file or malicious program in the Quarantine folder is securely isolated from other data on your computer and will not cause any harm or infect other files.

Quarantined malicious programs cannot be cleaned simply because they are programs. No virus is infecting a file, rather the entire program itself needs to be "cleaned". Any malicious programs that are quarantined should be deleted. View Virus logs to check whether a file is a Trojan or worm virus. Most Trojans can be identified by the name: TROJ_<name>, VBS_<name>, or JS_<name> and worms can be identified by: WORM_<name>.

For more information about how to handle files in the Quarantine Folder, view the interactive Quarantine Guide.

To view the Quarantine Guide:

1. On the PC-cillin Main window under the **Advanced** tab, click **Quarantine**.
2. Click **Quarantine Guide** and follow the instructions.

The default secondary action for Email Scan is Delete.

Important: If infected files that cannot be cleaned are important system files, a system error or failure to boot up the system may occur.

You can learn the virus type by viewing the Virus logs. The following provides further information about how to identify different types of viruses based on their name.

Type of malicious program	Name prefix	Examples
Trojan horses	JS_<name>, VBS_<name>, TROJ_<name>	TROJ_QAZ.A
Worms	WORM_<name>	WORM_KLEZ

Compressed files

While the Trend Micro scanning engine can detect viruses within compressed files, it cannot clean the files inside of a compressed archive beyond the second layer of compression. To clean a virus in a deeper layer of compression, you must first decompress the file. A compressed file that is compressed within another file is considered a compressed layer.

To clean a compressed file:

1. Disable the PC-cillin real-time scanning function so that it will not interfere with the decompression process.
2. Use an archive utility (for example, WinZip) to extract the files from the compressed file.
3. Make sure the PC-cillin real-time scanning function is enabled.
4. Run the main program. You can now manually scan and attempt to clean the infected files that were extracted in the second step.

Insufficient space or write-protected disks

By default PC-cillin creates a backup file, *.rb0 in the Backup folder (default location, C:\Program Files\Trend Micro\PC-cillin 2003\Quarantine\Backup), before attempting to clean an infected file. This is to make sure a back up exists if the infected file becomes corrupted during the cleaning process.

Sufficient disk space must be available for the backup files before attempting to clean the files.

If the disk is write-protected, make it writeable before attempting to clean the file.

Password-protected files

If a file is password-protected (for example, a password-protected ZIP or Word file), PC-cillin will not be able to detect or clean it. Please disable password-protection before attempting to scan or clean a file.

PE-type viruses

Since PE-type viruses (Portable Executable: standard Win32 file format) always stay in memory, the virus may not be completely cleaned. You can identify a PE-type virus by the virus name: PE_<name>.

To clean a PE-type virus:

1. Boot your computer with the rescue disk labeled Emergency Boot Disk (Disk 1).
2. Insert the PC-cillin rescue disk labeled PCSCAN Files Disk (Disk 2) into the A:\drive and at the DOS command prompt type:

```
A:\>PCSCAN /V/C
```

Follow the onscreen instructions. You can now start scanning and cleaning the viruses.

Note: If you do not have emergency rescue disks, refer to Creating rescue disks (for Windows 98, Windows Me operating systems only).

Creating Rescue Disks

Certain types of boot viruses can prevent your computer from booting normally. To clean these viruses, you need to start your computer from a clean disk and not the infected hard drive. A "rescue disk" is a bootable

floppy disk that PC-cillin can create if you are running Microsoft Windows 98 or Windows Me.

The PC-cillin rescue disks require a "pure DOS" environment to operate correctly, however Windows NT 4, 2000, XP no longer support a pure DOS environment.

For Windows NT 4, 2000, XP we recommend you create an Emergency Repair Disk. Refer to the Microsoft Windows documentation for instructions.

You need multiple disks to create the complete set of rescue disks.

Note: Rescue disks should be write protected after they are created. A disk is write protected when you can see through both squares in the upper corners.

- Emergency Boot Disk (Disk 1): Contains files necessary to start your computer. Use to start your computer if a boot virus has infected your computer and you cannot start your computer normally.
- PCSCAN Files Disk (Disk 2): Contains the scan engine. Use with the Pattern File disks to detect and clean viruses located in the boot sector of your computer.
- Pattern File Disks (Disks 3 and others): Contains pattern files to detect the latest viruses. Use with the PCSCAN Files disk to detect and clean viruses located in the boot sector of your computer.

Note: Do not restart your computer using rescue disks that were created for an earlier version of PC-cillin--this can result in data loss.

Before creating your rescue disks make sure you have a writing utensil to label the disks. You need at least seven disks to create a complete set of rescue disks.

If you've already got a set of rescue disks from a previous version of PC-cillin, you should create a new set after installing PC-cillin 2003. Likewise, if you created your rescue disks under Windows 98 and have upgraded to Windows Me, you need to create a new set of rescue disks. Of course, you can re-use your old floppies for the new disks. All data on the old disks will be lost in the creation of the new disks.

To create rescue disks:

1. Obtain some disks and insert one into the floppy drive of your computer.
2. Click **Start > Programs > Trend Micro PC-cillin 2003 > Create the Rescue Disks**. The Create Emergency Rescue Disks window appears.
3. Click **Complete Rescue Disk set**, and then **Click Next**.
4. Make sure the Target drive is correct and click **Next**. The Format dialog box appears.
5. Choose your format type (we recommend Full) and click **Start**. The disk starts formatting.
6. When the formatting is finished, click **Close**. The Format dialog box closes and PC-cillin starts copying the files to the disk.
7. As each floppy is finished, remove it and immediately label it. Slide up the plastic button in the upper left hand corner of the back of the disk to write protect it. The disk is write-protected when you can see through both squares in the upper corners. Creating the rescue disks takes about 10 minutes.
8. Repeat the procedure for each disk, starting from the formatting step.
9. Click **Finish**.

Note: You cannot make rescue disks on a machine infected with a boot virus. Be sure to clean (or delete) any viruses that have been detected.

Cleaning Boot Viruses

Boot sector viruses are especially troublesome (and dangerous) because they occupy a sensitive part of the hard drive, the boot sector, and load into memory whenever the system is started. From memory, they spread easily to any files that are subsequently opened and to floppy disks that are used.

To clean a boot virus:

1. Shut down your computer and turn off the power.
2. Insert the rescue disk labeled Emergency Boot Disk (Disk 1) in the floppy drive of your computer.

3. After waiting a few seconds, turn your computer on. Make sure your computer boots from the floppy drive. You may have to make changes to your computer's BIOS in order to boot from the floppy drive instead of the hard drive. Refer to your computer's manual or support Web site for detailed instructions how to perform this.
4. Insert the PCSCAN Files Disk (Disk 2), and then at the DOS prompt type the following:

```
pcscan /V /C
```
5. Press **Enter**.
6. When prompted, insert Pattern File Disk 1 and press **Enter**.
7. When prompted, insert the remaining pattern file disks in sequence and press **Enter**.

The last command tells PC-cillin to scan and clean all files on all drives, including the boot sector.

Note: Boot viruses spread easily. If PC-cillin detects a boot virus, it is very likely that one or more of your floppy disks are also infected. Be sure to run the Floppy Scan task and check all your floppies for viruses.

Understanding Viruses

Simply put, a computer virus is a program that replicates. To do so, it will need to attach itself to other program files (for example, .exe, .com, .dll) and execute whenever the host program executes. Beyond simple replication, a virus almost always seeks to fulfill another purpose: to cause damage.

Called the damage routine, or payload, the destructive portion of a virus can range from overwriting critical information stored on your hard disk's partition table to scrambling the numbers in your spreadsheets to just taunting you with sounds, pictures, or obnoxious effects.

To learn more about any particular virus, or about viruses in general, you can access the Trend Micro online Virus Encyclopedia or visit our Web site at:

www.trendmicro.com.

Understanding Trojans

Trojans, or Trojan horses, are small, seemingly harmless programs. To cause damage, these programs must be installed onto your system. Once installed, a Trojan has all the same privileges as the user of the computer and can exploit the system to do something the user did not intend. The main difference between a Trojan and a virus is that Trojans cannot replicate or spread on their own.



Guarding Against Internet Attacks

This chapter includes instructions on how to secure your Internet connection from malicious hackers. It also describes how to protect your computer from malicious Java or ActiveX programs or script viruses.

This chapter contains the following sections:

- Introducing the Personal Firewall on page 5-1
- Installing and Enabling the Personal Firewall on page 5-2
- Protecting Wi-Fi Connections on page 5-3
- Halting Internet Traffic on page 5-4
- Blocking Malicious Web Programs on page 5-5
- Filtering Unwanted Web Content on page 5-6

Introducing the Personal Firewall

The PC-cillin 2003 Personal Firewall protects your computer against attacks from the Internet. A firewall creates a barrier between your computer and the network (LAN, Internet). This barrier examines and filters the incoming and outgoing Internet traffic. By filtering Internet traffic, the firewall helps prevent malicious hackers from invading your computer and causing mischief.

The PC-cillin 2003 is a stateful inspection firewall which means it can track and monitor the state of each connection to make sure nothing strange is going on, for example, stateful inspection would know if something other

than HTTP was running over port 80. A stateful inspection firewall keeps track of each "session" and knows if the session is already active. The firewall uses this information plus a list of rules to determine if packet is blocked or forwarded.

Filtering decisions are based not only on defined rules, but also on context that has been established by prior packets that have already passed through the firewall.

The Personal Firewall includes the following features:

- Ability to allow or deny traffic based on a specified port or protocol
- Dynamic outgoing access warning appears when a program that is not included in the Exception list tries to connect to the Internet (High security level only)- this warning helps prevent unauthorized programs such as a Trojans from stealing data or someone remotely controlling your computer
- Intrusion Detection System prevents known firewall attacks (such as *Too big fragment*, *Overlapping fragment attack*, *Tiny fragment attack*)
- Prevents Trojan damage by closing particular ports that are known to be used in attacks
- Provides updateable firewall and IDS rules
- Ability to filter HTTP strings from server-to-server to prevent hybrid attacks like Nimda and Code Red

Installing and Enabling the Personal Firewall

If you didn't install the Personal Firewall during setup, you can easily add it from the Start menu. Before installing the Personal Firewall, make sure the PC-cillin Main and Settings windows are closed and are not opened during the installation process.

To install the Personal Firewall:

1. Click **Start > Programs > Trend Micro PC-cillin 2003 > Add or Remove Personal Firewall**.
2. Click **Install**.
3. Click **Close**.

Enable your Personal Firewall so you can connect to the Internet without worrying about someone invading your computer. The Personal Firewall protects you against hackers trying to damage files, steal personal information, or create mischief.

To enable the Personal Firewall:

1. On the Settings window, click **Personal Firewall > Security Level**.
2. Select the **Enable Personal Firewall** check box. If you are on a secure LAN select the **Allow my computer...** check box to make your computer visible to other network users.
3. Click **Apply**.

Protecting Wi-Fi Connections

PC-cillin provides a simple way to set your Personal Firewall settings to the level that provides the best mix of security and flexibility when connecting to a wireless Ethernet.

Wireless Ethernet, also called wireless fidelity (Wi-Fi), allows connectivity between laptops or other portable computing devices and LANs without the need for a physical connection. However, this convenience also involves a risk of intrusion especially when accessing unknown wireless networks.

Important: You must have installed the Personal Firewall to use this feature.

To protect Wi-Fi connections:

- On the PC-cillin Main window under the **Advanced** tab, click **Internet Traffic Control**, and then click **Wi-Fi Protection**. To disable Wi-Fi Protection, click **Wi-Fi Protection** again.

Tip: In the system tray, right-click the Real-time agent icon and click **Wi-Fi Protection**.



Wi-Fi Protection enabled



**Wi-Fi Protection disabled
(default)**

Note: While Wi-Fi Protection is enabled, Personal Firewall settings are locked.

Halting Internet Traffic

Complete control over your Internet traffic is vital for virus outbreaks or other intrusion attacks. Halting Internet traffic immediately stops all incoming and outgoing Internet traffic and is particularly useful during times when someone is trying to remotely break into your computer or there is a virus outbreak.

Important: You must have installed the Personal Firewall to use this feature.

To halt Internet traffic:

- On the PC-cillin Main window under the **Advanced** tab, click **Internet Traffic Control**, and then click **Halt Internet Traffic!**. To allow Internet traffic, simply click **Halt Internet Traffic!** again.

Tip: In the system tray, right-click the Real-time agent icon and click **Halt Internet Traffic** or when Real-time Scan detects a virus simply click **Halt Internet Traffic!** on the message box that appears.



Internet Traffic allowed (default)



Internet Traffic blocked

Blocking Malicious Web Programs

PC-cillin WebTrap blocks malicious scripts (Java and ActiveX programs) while you are viewing Web pages while allowing harmless ones to safely pass through. Although most Web sites are completely harmless, it is possible for someone to create a small program and set it to run invisibly whenever their Web page is accessed. These programs may destroy data, steal your passwords, financial data, etc.

To block malicious Web programs:

1. On the Settings window, click **Internet Security > WebTrap**.
2. Select the **Enable WebTrap** check box.
3. Click **Apply**.

WebTrap and the Personal Firewall

WebTrap protects you against malicious scripts (Java or ActiveX programs) while still allowing the harmless ones to pass through safely. The Personal

Firewall makes your computer's entry points invisible to snooping intruders and creates a barrier between your computer and the network (LAN, Internet). This barrier examines and filters network traffic to your computer. By filtering network traffic, the firewall prevents malicious programs or files from entering your computer.

Filtering Unwanted Web Content

For protection against offensive Web content, PC-cillin offers the Site filter. This feature lets you set whatever Web sites you want "off-limits" to other users of the computer. Site filter is especially useful for families where many members share a single computer.

To filter unwanted Web content:

1. On the Settings window, click **Internet Security > Site Filter**.
2. Select the **Enable Site filter** check box.
3. If you want to allow entry to restricted Web sites after providing a warning, select the **Permit access...** check box. If this check box is not selected, any Web site in the Restricted Sites list will not load and a message will appear in the browser notifying the user they are trying to access a restricted site.
4. Click **Apply**.

Tip: If you selected the **Extend to all sub-pages** and **Permit access after being prompted** check boxes, each time you view a page on the Web site you will be prompted. To prevent this, leave the **Extend to all sub-pages** check box clear when adding a new site.



Getting Support

Trend Micro is committed to providing service and support that exceeds our user's expectations regardless of their location. This chapter contains information on how to get technical support. Remember, you must register your product to be eligible for support.

The following topics are discussed in this section:

- Before Contacting Technical Support on page 6-1
- Visiting the Trend Micro User's page on page 6-2
- Visiting the Technical Support Web site on page 6-2
- Contacting Technical Support on page 6-2
- TrendLabs™ on page 6-3

Before Contacting Technical Support

Check your documentation: the manual and online help provide comprehensive information about PC-cillin. Search both documents to see if they contain your solution.

Visit our Technical Support Web site: our Technical Support Web site contains the latest information about all Trend Micro products. Previous user inquiries that have been answered are posted on the support Web site.

Visiting the Trend Micro User's page

Built exclusively for Trend Micro users, visit the Trend Micro user's page to receive the latest news about PC-cillin. As a registered user, you can access information that is not available outside this Web site.

To visit the Trend Micro User's page:

- On the PC-cillin Main or Settings window, click **Help > Trend Micro User Home Page**.

Visiting the Technical Support Web site

Visit the Trend Micro Technical Support Web site to find answers to your inquiries. The Trend Micro Technical Support Web site contains the latest updated information about our products.

To visit the Technical Support Web site:

- On the PC-cillin Main or Settings window, click **Help > Technical Support Home Page**.

Contacting Technical Support

A license to Trend Micro antivirus software includes the right to receive pattern file updates and technical support from Trend Micro or an authorized reseller, for one (1) year. Thereafter, you must renew Maintenance on an annual basis at Trend Micro's then-current Maintenance fees to have the right to continue receiving these services.

To speed up your problem resolution, when you contact our staff please provide as much of the following information as you can:

- Product serial number
- PC-cillin program, scan engine, pattern file, version number
- OS name and version and Internet connection type
- Exact text of any error message given
- Steps to reproduce the problem

The best way to receive support is to send an email to our highly trained Technical Support staff or visit our Web site.

Email: pc-cillin@support.trendmicro.com

For other ways to contact PC-cillin Technical Support, check the "Support" section of our Web site at:

URL: www.pc-cillin.com

TrendLabs™

Trend Micro TrendLabs is a global network of antivirus research and product support centers that provide continuous 24 x 7 coverage to Trend Micro customers around the world.

Staffed by a team of more than 250 engineers and skilled support personnel, the TrendLabs dedicated service centers in Paris, Munich, Manila, Taipei, Tokyo, and Irvine, CA. ensure a rapid response to any virus outbreak or urgent customer support issue, anywhere in the world.

The TrendLabs modern headquarters, in a major Metro Manila IT park, has earned ISO 9002 certification for its quality management procedures in 2000 - one of the first antivirus research and support facilities to be so accredited. We believe TrendLabs is the leading service and support team in the antivirus industry.

For more information about TrendLabs, please visit:

www.trendmicro.com/en/security/trendlabs/overview.htm



Appendix

Appendix

This appendix contains important information that may not necessarily be applicable for all users. It includes the following sections:

- Upgrading Your Trial Version Software on page Appendix-1
- Installing PC-cillin for Wireless on page Appendix-2
- Enabling and Configuring Proxy Settings on page Appendix-4
- Removing PC-cillin on page Appendix-5
- Removing PC-cillin for Wireless on page Appendix-5

Upgrading Your Trial Version Software

Upgrading your 30-day trial version to the full version of the software and registering enables you to use the full functionality of PC-cillin 2003.

In addition, after you upgrade your software and register online, you receive the following benefits: the right to receive pattern file updates and technical support from Trend Micro or an authorized reseller, for one (1) year. Thereafter, you must renew Maintenance on an annual basis at Trend Micro's then-current Maintenance fees to have the right to continue receiving these services.

If you continue to use the trial version after 30 days all functions are disabled.

To upgrade your trial version software:

1. On the PC-cillin Main window, click **Register**. The **Register Now** screen appears.

2. Under **Step 1** on the **Register Now** screen, type your serial number.
3. Click **Upgrade Now**.

You have upgraded your trial version software to the full version. You should now continue and register your software.

Installing PC-cillin for Wireless

As PDAs and other handheld computing devices increase the number of ways to communicate with other devices, the chance of becoming infected also increases. These days it is common for PDAs to feature Internet connectivity.

PC-cillin for Wireless provides portable, easy-to-use antivirus security for wireless devices to defend against potential threats. Malicious code and other unique threats hidden inside files, email, or on the Web can enter your Palm, Pocket PC, or EPOC device during beaming, synchronization, or Internet access.

To install PC-cillin for Wireless:

1. Insert the PC-cillin program CD into your CD-ROM drive, and do the following:
 - If the menu automatically appears, click **Install PC-cillin for Wireless**.
 - If the installation program doesn't automatically start, click **Start > Run**. In **Open**, type D:\autorun.exe and click **OK** (where D:\ is the drive letter of your CD-ROM). Click **Install PC-cillin for Wireless**.

The PC-cillin for Wireless folder opens and the PC-cillin for Wireless readme file appears.
2. Follow the relevant instructions for your PDA type.

For Palm™ OS

1. Make sure your Palm device is securely seated in the cradle and attached to the desktop.
2. Open the Palm Desktop application, then click **Install**.

3. In the Install Tool window, click the **User** list, and select the name that corresponds to your organizer.
4. Click **Add**, then multi-select scan.prc (main program), Pattern_<XXX>.prc (XXX represents pattern file number), and RealTime.prc (the real-time scan module) from the list box. Click **Open** to add the file, or **Cancel** to abort the operation. The required files appear in the Install Tool window.
5. Click **Done**. The Install Tool dialog box appears.
6. Click **OK** to proceed with installation during the next HotSync operation, or **Cancel** to abort the operation.
7. Insert your Palm OS platform device in the cradle and press the "HotSync" button.

For EPOC

1. Make sure the EPOC device is connected to the Desktop.
2. Double-click the PcciEpoc.SIS icon to establish a connection between the device and your PC. The Select disk window appears.
3. Click **Next** to start the installation. The **Installing PC-cillin for EPOC** window opens. To abort installation, click **Cancel**.
4. At the **EPOC Install - PC-cillin for EPOC** window, click **Finish** to complete the installation.

For Pocket PC

1. Make sure the Pocket PC device is connected to the desktop and Microsoft ActiveSync™ is running.
2. Locate the package that corresponds to your CPU type. The packages currently available are:
 - PC-cillin for Pocket PC_ARM (Compaq iPAQ; Strong ARM CPU)
 - PC-cillin for Pocket PC_MIPS (Casio Cassiopeia)
 - PC-cillin for Pocket PC_SH3 (HP Jornada)
3. Double-click the appropriate package's icon. The **PC-cillin for Pocket PC - Installation Folder** window opens.

4. Specify the destination for the installation files. The default destination is the Windows temp directory.
5. Click **Finish** to continue. The Installing Applications dialog box opens. Click **Yes** to install PC-cillin in the default application directory, click **No** to specify an alternative, or **Cancel** to abort the operation.

Enabling and Configuring Proxy Settings

A proxy server is used to provide security and increase efficient use of network bandwidth. Most home users do not use a proxy server, but many offices, schools, and Internet Service Providers do. If you are having trouble connecting to the Internet to register, or download program updates, it may be because you use a proxy server but it has not been identified or there is an error in the address/credentials.

If you use a proxy server on your network you need to enter the IP address (number) and port of this proxy server.

In addition, if you use a proxy server and users are required to log on, you need to supply the appropriate logon credentials.

To enable and configure proxy settings:

1. On the Settings window, click **Program Update**.
2. Under **Proxy information**, select the **Use a proxy server...** check box.
3. Click **Proxy Settings**, and then do the following.
 - In **Proxy address**, type the IP address of the proxy server or domain name (for example, proxy.yourcompany.com).
 - In **Port**, type the port number of the proxy server (for example, 80).
 - In **User name** and **Password**, type your proxy server logon credentials.
4. Click **OK**.
5. Click **Apply**.

Removing PC-cillin

Before removing PC-cillin, you must close all other open applications and stop Real-time Scan. To halt real-time scanning, right-click the PC-cillin Real-time agent in the system tray, and then click Real-time agent to clear the check. The lightning bolt icon turns gray when Real-time Scan is disabled.

During uninstallation, PC-cillin deletes all quarantined files. These files may contain viruses and should not be left on your computer. If you must preserve them, we suggest that before uninstallation you restore the files to a safe, isolated, location such as a specially marked floppy disk.

To remove PC-cillin:

- Click **Start > Programs > Trend Micro PC-cillin 2003 > Uninstall PC-cillin 2003**. Click **Yes** to remove PC-cillin.

Removing PC-cillin for Wireless

The following instructions tell you how to remove PC-cillin for Wireless from your PDA depending on the platform.

For Palm OS

1. Select **Delete** from the Palm system menu. The Delete list appears.
2. Remove the following files:
 - PC-cillin - the main program file
 - PATTERN.xxx - the pattern file
 - Pccillin.log - the log file; this contains log information
 - RealTime - the real-time scanning module
3. Tap **Done** to return to the main screen.

For Pocket PC

1. Tap **OK** at the top-right corner of the screen to close PC-cillin for Pocket PC.
2. Click **Start > Settings**. The Settings dialog box appears.

3. Select the **System** tab, and then tap the **Remove Programs** icon.
4. Select the Trend Micro PC-cillin for Pocket PC item, then click **Remove**. The Remove Program dialog box opens.
5. Tap **Yes** to remove the program.

For EPOC

1. Click **ESC** to close the PC-cillin for EPOC program.
2. Click **Control Panel** on the right-hand side bar.
3. Double-tap the **Add/remove** icon. The Installed Programs dialog box appears.
4. Select the **PC-cillin for EPOC** item, and then tap **Remove**. A confirmation dialog box opens. Tap **Yes** to remove the program.